

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Hidehiko FUJIWARA, et al.
Title: COMMUNICATION SYSTEM WITH FUNCTION OF
ENCIPHERMENT/DECIPHERMENT BY AGENCY
Appl. No.: Unassigned
Filing Date: 11/25/2003
Examiner: Unassigned
Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

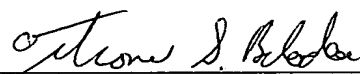
In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2002-348068
filed November 29, 2002.

Respectfully submitted,

Date: November 25, 2003

FOLEY & LARDNER
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By  Reg. No. 43438
for David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 2 9 日
Date of Application:

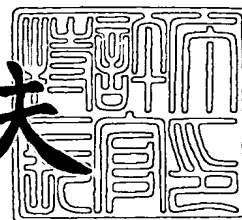
出 願 番 号 特 願 2 0 0 2 - 3 4 8 0 6 8
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 4 8 0 6 8]

出 願 人 N E C インフロンティア株式会社
Applicant(s):

2 0 0 3 年 1 0 月 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 8 2 8 6 7

【書類名】 特許願

【整理番号】 22400200

【提出日】 平成14年11月29日

【あて先】 特許庁長官 殿

【国際特許分類】 H04K 1/00
H04L 9/00

【発明者】

【住所又は居所】 神奈川県川崎市高津区北見方 2 丁目 6 番 1 号 エヌイー
シーインフロンティア株式会社内

【氏名】 藤原 秀彦

【発明者】

【住所又は居所】 神奈川県川崎市高津区北見方 2 丁目 6 番 1 号 エヌイー
シーインフロンティア株式会社内

【氏名】 小林 佳和

【特許出願人】

【識別番号】 000227205

【氏名又は名称】 エヌイーシーインフロンティア株式会社

【代理人】

【識別番号】 100065385

【弁理士】

【氏名又は名称】 山下 穰平

【電話番号】 03-3431-1831

【手数料の表示】

【予納台帳番号】 010700

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0110263

【プルーフの要否】 要

【書類名】 明細書
【発明の名称】 通信システム
【特許請求の範囲】

【請求項 1】 ファイアウォールで保護されたイントラネット内の子機と、前記ファイアウォールの外側の子機とがインターネットを介して通信を行うシステムにおいて、前記イントラネット内に代理通信部を設け、前記代理通信部が前記イントラネット内の暗号化の仕組みを持たない子機の代理で暗号化又は非暗号化を行うことを特徴とする通信システム。

【請求項 2】 前記代理通信部は、暗号化されたデータを解析して Web アクセスであるか、暗号化された構内 IP 電話通信であるかを判別し、判別結果に基づいて Web サーバー又はイントラネット内の子機への通信を行うことを特徴とする請求項 1 に記載の通信システム。

【請求項 3】 前記代理通信部は、前記ファイアウォールの外側からの暗号化に非対応の子機からのアクセスである時は、暗号化無しで通信を行うことを特徴とする請求項 1 に記載の通信システム。

【請求項 4】 前記代理通信部は、前記子機の機能及び前記ファイアウォールを越えるための音声とデータの形式を変換する機能を有する仮想子機を有し、当該仮想子機が代理で通信を行うことを特徴とする請求項 1 に記載の通信システム。

【請求項 5】 前記代理通信部は、前記ファイアウォールの内側の子機からファイアウォールの外側の暗号化非対応端末へのアクセスである時には、暗号化なしで通信を行う、又は通信を許可しないことを特徴とする請求項 1 に記載の通信システム。

【請求項 6】 前記イントラネット内の子機とインターネット上の子機との通信は、前記ファイアウォールの HTTP ポートを通して行うことを特徴とする請求項 1 に記載の通信システム。

【請求項 7】 暗号化の仕組みを有する子機を用い、当該子機は前記ファイアウォールの内側と外側のどちらに在るかを判断する手段を有し、その判断結果に基づいて前記ファイアウォールの外側に在る時は暗号化を行い、前記ファイア

ウォールの内側にいる時には暗号化機能を停止することを特徴とする請求項 1 に記載の通信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、インターネットを用いて通信を行う通信システムに関し、特に、イントラネット内部に構内 I P 電話システムを構築する場合の技術に関するものである。

【0 0 0 2】

【従来の技術】

従来、イントラネットとインターネットの間に強固な F i r e w a l l （ファイアウォール）を構築することは、例えば、社内情報ネットワーク上で一般的に普及している。そのようなファイアウォールで保護されたイントラネットの内部に構内 I P 電話を構築する場合には、通信の相互接続性を確保するため、或いは通信帯域を削減するため、極力暗号化は行わずに、通常の R T P 接続を用いて音声通信を行うことが望ましい。

【0 0 0 3】

ところで、従来の通信システムとしては、例えば、特開 2 0 0 1 - 2 3 7 8 8 8 や特開平 1 1 - 2 8 4 7 2 6 号公報に記載されたシステムがある。特開 2 0 0 1 - 2 3 7 8 8 8 には、音声データに対して秘匿処理を施すことが記載されている（特許文献 1 参照）。また、特開平 1 1 - 2 8 4 7 2 6 号公報には、発呼者が電子メール等の送信者と電話で話すことを望む場合、発呼者のコンピュータ上の相手方の情報を使用して自動的に音声接続を行うシステムが記載されている（特許文献 2 参照）。

【0 0 0 4】

【特許文献 1】

特開 2 0 0 1 - 2 3 7 8 8 8 （段落 0 1 6 1 ～ 0 1 6 4）

【特許文献 2】

特開平 1 1 - 2 8 4 7 2 6 号公報（段落 0 0 1 7 ～ 0 0 2 0）

【0005】**【発明が解決しようとする課題】**

前述のようにイントラネット内部に構内 IP 電話を構築する場合、暗号化を行わずに通常の RTP 接続を用いて音声通信やデータ通信を行うと、ファイアウォールの外側に移動した子機との通信は暗号化が行われないうえ、子機からの音声と数値データがインターネット上の第三者に盗み取られてしまう可能性がある。そこで、単純な暗号化を行うとすると、イントラネット内の全ての子機で暗号化を扱うための機能追加を行う必要があるため、相互接続性が低下し、通信帯域が増加してしまう。また、もしも子機側の改造が不可等の理由で暗号化に対応できない場合には、通信が行えなくなる問題があった。

【0006】

また、上記特開 2001-237888 や特開平 11-284726 号公報には、音声データ等の通信を行うシステムが開示されているが、いずれのシステムも前述のような課題を解決するものではなかった。

【0007】

本発明は、上記従来の問題点に鑑みなされたもので、その目的は、イントラネット内の子機が暗号化の仕組みを持たなくても、確実に通信を保護することが可能な通信システムを提供することにある。

【0008】**【発明を解決するための手段】**

本発明は、上記目的を達成するため、ファイアウォールで保護されたイントラネット内の子機と、前記ファイアウォールの外側の子機とがインターネットを介して通信を行うシステムにおいて、前記イントラネット内に代理通信部を設け、前記代理通信部が前記イントラネット内の暗号化の仕組みを持たない子機の代理で暗号化又は非暗号化を行うことを特徴とする。

【0009】**【発明の実施の形態】**

次に、本発明の実施の形態について図面を参照して詳細に説明する。図 1 は本発明の一実施形態を示すブロック図である。図 1 において、101 は子機、10

2 はインターネット、103 はイントラネット、104 はイントラネット 103 を保護するファイアウォール (Firewall) である。イントラネット 103 内には、イントラネット 103 上に常駐し、代理で暗号化／非暗号化を行う代理通信部 105 が設けられている。子機 101 はインターネット 102 上の子機であり、暗号化の仕組みを有するものとする。

【0010】

また、109、110 はイントラネット 103 内の子機、111 はイントラネット 103 内の Web サーバーである。子機 109、110 は暗号化の仕組みを持たないものとする。112 はインターネット 102 上の暗号化に対応していない非対応端末である。

【0011】

代理通信部 105 は HTTP 通信制御部 106、暗号制御部 107、仮想子機 108 を含んでいる。代理通信部 105 内の暗号制御部 107 はファイアウォール 104 で保護されていないインターネット 102 上の子機 101 への通信を暗号化し、その内容の保護を行う。即ち、暗号化の仕組みを持たない子機 109 や子機 110 の代わりに暗号化を行う。また、ファイアウォール 104 の外側の暗号化の仕組みを有する子機 101 からの通信に対し、代理通信部の暗号制御部 107 が代理で非暗号化を行い、ファイアウォール 104 の内側の子機 109 や子機 110 と通信を行う。

【0012】

この際、代理通信部 105 は通信を開始する場合のネゴシエーション時において、互いに通信相手の情報に基づいて暗号化に対応する端末であるか、どの種類の暗号であるか等を判断する。従って、この判断結果に基づいて、ファイアウォール 104 の外側の子機 101 から内側の子機 109 や子機 110 へのアクセス時には、非暗号化を行い、逆に、子機 109 や子機 110 から子機 101 へのアクセス時には、暗号化を行う。

【0013】

また、ファイアウォール 104 内の子機 109 や子機 110 からファイアウォール 104 の外側の子機 101 へのアクセス時には、子機 101 は暗号化対応端

末であるので暗号化を行い、子機 109 や子機 110 から非対応端末 112 へのアクセス時には、暗号化しないで通信を行う。また、この際、通信を許可しないようにしてもよい。

【0014】

本実施形態では、このように代理通信部 105 が代理で暗号化／非暗号化を行うことによって、ファイアウォール 104 の内側にいる子機 109 や子機 110 が暗号化・非暗号化を行う必要がないため、暗号の仕組みを持たない子機とも共存できるように構成されている。そのため、接続性の高い構内 IP 電話システムを構築することが可能である。

【0015】

また、代理通信部 105 には仮想子機 108 が設けられている。この仮想子機 108 は、ファイアウォール 104 の内側の子機 109 や子機 110 の機能、及びファイアウォール 104 を越えるための音声とデータの形式を変換する機能（例えば、HTTP パケット形式に読み替える機能）を持っている。従って、子機 101 と、子機 109 や子機 110 とが通信を行う場合、子機 109 や子機 110 から見ると、実際には子機 101 と通信しているが、仮想子機 108 が見えており、子機 101 から見ると仮想子機 108 が見えており、仮想子機 108 が代理で通信を行う。

【0016】

このように仮想子機 108 が代理で通信を行うことにより、ファイアウォール 104 によって保護されているイントラネット 103 にある全ての子機 109 や子機 110 は、特別な仕組みを要することなく、RTP といった暗号化されていない標準的なデータ形式で通信を行うことが出来る。このデータ通信を図 1 の子機 101 との秘匿通信で示す。そのため、一般的な構内 IP 電話機との接続性を保証している。

【0017】

また、イントラネット 103 内の子機 109 や子機 110 が暗号化の仕組みを持つことが出来なくても、仮想子機 108 と暗号制御部 107 を通してファイアウォール 104 の外にある子機 101 と秘匿通信を行うことが出来る。また、代

理通信部 1 0 5 内における暗号制御部 1 0 7 は暗号化されたデータを解析する機能を有し、これが W e b アクセスであるか、暗号化された構内 I P 電話通信であるかを判断する。

【 0 0 1 8 】

H T T P 通信制御部 1 0 6 は、その判断結果に基づいて W e b アクセスである時は W e b サーバー 1 1 1 へ、暗号化された構内 I P 電話通信である時には、通信相手の子機 1 0 9 或いは子機 1 1 0 への通信を行うように制御する。本実施形態では、W e b アクセスであるか、構内 I P 電話通信であるかを判断し、ファイアウォール 1 0 4 の H T T P 経由（ファイアウォール 1 0 4 の 1 つのポート）のアクセスを管理できるため、ファイアウォール 1 0 4 の安全性を確かめることが出来る。

【 0 0 1 9 】

一方、ファイアウォール 1 0 4 の外側の子機 1 0 1 はネットワーク特性検出部 1 1 3、暗号制御部 1 1 4、H T T P 通信制御部 1 1 5 を含んでいる。ネットワーク特性検出部 1 1 3 は通常の R T P 通信が行えるかどうかを判断する等の方法でネットワークの接続環境を判断し、現在、子機 1 0 1 がファイアウォール 1 0 4 の内側にいるのか、外側にいるのかを判別する。

【 0 0 2 0 】

この判別結果に基づいて暗号制御部 1 1 4 の動作が切り換えられ、子機 1 0 1 がファイアウォール 1 0 4 の外側にいる場合には、暗号化を行い、子機 1 0 1 が内側にいる場合には、暗号化を行わないように制御を行う。このように子機 1 0 1 のファイアウォール 1 0 4 の内側、外側の位置に応じて暗号化／非暗号化を切り換えることにより、子機 1 0 1 のファイアウォール 1 0 4 の内側、外側によらず他装置との接続性を向上することが出来る。特に、子機 1 0 1 がファイアウォール 1 0 4 の外側にいる場合には、ユーザーはそれを意識することなく、自動的に秘匿通信に切り換えることが可能である。

【 0 0 2 1 】

また、非対応端末 1 1 2 のように子機がこの仕組みを持たない場合でも、暗号制御部 1 0 7 は R T P パケットの内容を解析する機能を有しており、前述のよう

に通信を開始する場合のネゴシエーション時に暗号化に非対応の端末 112 からのアクセスであることを確認すると、仮想子機 108 が暗号化無しで代理通信を行うため、暗号化に対応していない端末 112 においても接続性を確保することが出来る。

【0022】

ここで、ネットワーク管理者はこの代理通信部 105 を、例えば、自宅や会社のイントラネット 103 に予め配置しておくことにより、子機 101 を持ってさえいれば、ファイアウォール 104 の内外に拘わらず、秘匿通信を行うことが出来る。更に、ファイアウォール 104 の内側に存在する装置は、個別に暗号化するための機構を用意することなく、ファイアウォール 104 の外側の子機 101 と秘匿通信を行うことが出来る。

【0023】

次に、本実施形態の動作を図 2 に示すフローチャートを参照して説明する。なお、ファイアウォール 104 の外側からの秘匿通信時の動作を説明する。図 2 において、まず、子機 101 において音声・数値データを取得し（ステップ 201）、ネットワーク特性検出部 113 が前述のように通常の RTP 通信を行えるかどうかを判断する等の方法でネットワークの接続環境を判断し、子機 101 がファイアウォール 104 の内側にいるのか、外側にいるのかを判断する（ステップ 202）。この時は、子機 101 はファイアウォール 104 の外側にいると判断したものとする。

【0024】

次いで、子機 101 内における暗号制御部 114 が暗号化を行い（ステップ 203）、そのパケットを HTTP 通信制御部 115 が HTTP パケット化して（ステップ 204）、インターネット 102 に送出する（ステップ 205）。この HTTP パケットはファイアウォール 104 の HTTP ポートを経由して、代理通信部 105 の HTTP 通信制御部 106 で取得され（ステップ 206）、前述のようにネゴシエーション時において暗号化制御部 107 ではその HTTP パケットが暗号化された音声・数値データかどうかを判断し、HTTP 通信制御部 106 ではその判断結果に基づいてその他の Web アクセスと区別、分離を行う（

ステップ207)。

【0025】

この時は、暗号化されたHTTPパケットであるので、代理通信部105のHTTP通信制御部106が非HTTPパケット化し、更に、暗号制御部107が非暗号化を行う(ステップ208)。非暗号化された音声・数値データは仮想子機108により代理で送信され(ステップ209)、子機109或いは子機110により再生される(ステップ210)。

【0026】

また、ファイアウォール104の内側の子機109や子機110からファイアウォール104の外側の子機101と通信を行う場合には、ネゴシエーション時において通信相手の子機101は暗号化に対応の子機であると判断し、代理通信部105の仮想子機108が代理で通信を行い、暗号制御部107が音声・数値データの暗号化を行う。

【0027】

また、HTTP通信制御部106がHTTPパケット化を行い、このHTTPパケットはファイアウォール104のHTTPポートを経由してインターネット102上に送出され、子機101で受け取られる。子機101のHTTP通信制御部115では非HTTPパケット化を行い、暗号制御部114では非暗号化を行う。

【0028】

更に、ファイアウォール104の内側の子機109や110からファイアウォール104の外側の非対応端末112への通信を行う場合には、代理通信部105はネゴシエーション時において通信相手は暗号化に非対応であると判断し、この時は暗号化しないで通信を行う。また、前述のように通信を許可しないようにすることも可能である。

【0029】

【発明の効果】

以上説明したように本発明は、次の効果がある。

【0030】

(1) 代理通信部が代理で暗号化／非暗号化を行うことにより、イントラネット内における全ての子機の暗号化の対応が不要となり、暗号の仕組みを持たない子機でも、暗号化されたファイアウォール外の子機とそのまま秘匿通信を行うことが出来る。

【0031】

(2) 管理の及ばないインターネットの途中経路では接続性を保証できないVPN等の暗号化ツールと比べて、ファイアウォールのHTTPポートを通すこの方法は高い接続性を実現することが出来る。

【0032】

(3) パケットの内容を解析することで、通常のWebアクセスと構内IP電話通信とを区別することが出来るので、ファイアウォールのHTTPポートを通過するパケットを監視することが可能となり、安全性が向上する。

【0033】

(4) ネットワーク特性検出部が子機の位置がファイアウォールの内側が外側を判断し、それに基づいて暗号化／非暗号化を切り換えることにより、ファイアウォールの外側では秘匿通信が行え、内側にいる場合には接続性を確保することができる。

【0034】

(5) ファイアウォールの外側の暗号化に非対応の端末からも接続を保証することが出来る。

【図面の簡単な説明】

【図1】

本発明の一実施形態を示すブロック図である。

【図2】

図1の実施形態の動作を示すフローチャートである。

【符号の説明】

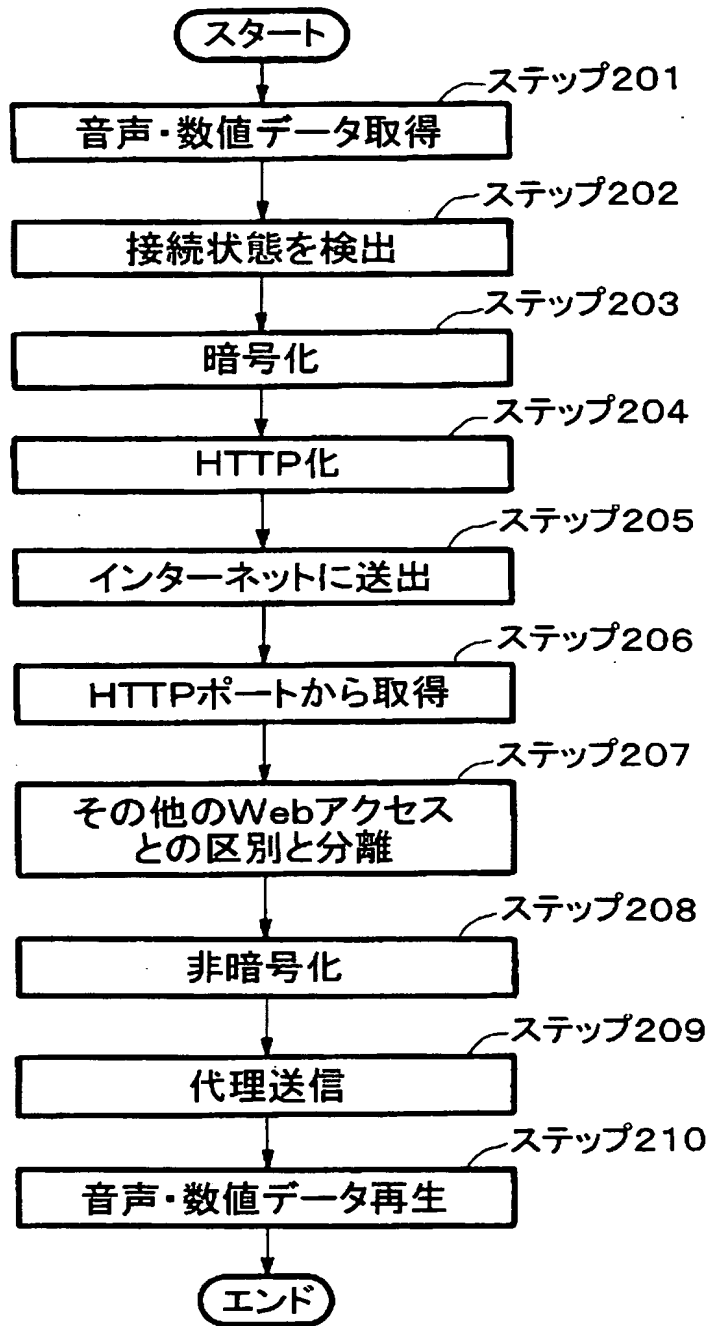
101 子機

102 インターネット

103 イントラネット

- 1 0 4 ファイアウォール
- 1 0 5 代理通信部
- 1 0 6 H T T P 制御部
- 1 0 7 暗号制御部
- 1 0 8 仮想子機
- 1 0 9、1 1 0 子機
- 1 1 1 W e b サーバー
- 1 1 2 非対応端末
- 1 1 3 ネットワーク特性検出部
- 1 1 4 暗号制御部
- 1 1 5 H T T P 制御部

【図 2】



【書類名】 要約書

【要約】

【課題】 ファイアウォールで保護されたイントラネット内に構内 I P 電話を構築する場合、イントラネット内の全ての子機が暗号化の仕組みの機能追加を必要とし、相互接続性等が低下する。

【解決手段】 イントラネット 1 0 3 内に代理通信部 1 0 5 を設け、ファイアウォール 1 0 4 の外側のインターネット 1 0 2 上の子機 1 0 1 と通信を行う場合には、代理通信部 1 0 5 がイントラネット 1 0 3 内の暗号化の仕組みを持たない子機 1 0 9 や子機 1 1 0 の代わりに代理で暗号化又は非暗号化を行う。また、子機 1 0 1 はファイアウォール 1 0 4 の内側にいるか外側にいるかを判断し、外側にいる時は暗号化を行い、内側にいる時は暗号化を行わないようにする。

【選択図】 図 1

特願 2002-348068

出願人履歴情報

識別番号

[000227205]

1. 変更年月日 2001年 6月 4日
[変更理由] 名称変更
住 所 神奈川県川崎市高津区北見方2丁目6番1号
氏 名 エヌイーシーインフロンティア株式会社
2. 変更年月日 2003年 7月30日
[変更理由] 名称変更
住 所 神奈川県川崎市高津区北見方2丁目6番1号
氏 名 NECインフロンティア株式会社